VOILA ! DOUBLE -=V=- et COUCOU77 Sont heureux de vous faire profiter de ce TUTO, faites en bon usage !!!!!

1. Quelques termes techniques indispensables avant de commencer (langage utiliser par les teams) :

FTP : ftp signifie "File Transfer Protocol".
Protocole par lequel on peut envoyer ou recevoir des fichiers (Upload, Download).

PUB : Pub signifie public.
C'est un serveur FTP qui peut se trouver n'importe où dans le monde
Ca regroupe tous les serveurs FTP avec accès anonyme. (ce sont les serveurs qui nous intéressent)

IP : Pour simplifier, c'est l'adresse attribué à un périphérique reseau (noeud) et qui permet son identification sur le net. Elle peut être attribuée dynamiquement ou statiquement. Elle est composée de 4 champs codés chacun sur 8 bits.

RACINE : Racine correspond au répertoire à la base, le répertoire racine …
En générale "/" Pour les serveurs avec accès en écriture dans un sous répertoire on parle de : "/nom_du_répertoire/" (/public/ , /vti_pvt/ …)

PATH : C'est le chemein composé de l'arborescence de répertoires qui se trouve sur le serveur c'est le chemin pour parvenir au fichier que vous avez upper sur le ftp.

format : DIVX : ce sont des dvd compressés.

format : MP3 : c'est des music compressées.

SCREENER : c'est un film pris avec une cam numérique dans un cinéma.

APPZ : ça veut dire application donc programmes.

ERREUR 421 : cela signifie que tu ne peux pas te connecter au ftp pour le moment vu qu il y a trop de monde.

Reply : Le reply est un élément très important de tout bon "boarder" qui se respecte. En effet cela permet de faire vivre la Board, tout en remerciant les uploaders pour leur boulot ; mais aussi pour avoir une précision sur quelque chose ou faire passer un message. Sur beaucoup de boards votre statut change en fonction du nombre de replys que vous envoyez, ceci afin de voir si vous êtes actifs ou pas.

POSTER : c'est faire un up sur un ftp et le mettre sur un board à disposition des membres.

SCANNER : c'est trouver des ftp libre où l'on peut upper c'est le but de ce tutorial quand on scan on utilise un logiciel qui va chercher des ports en écoute sur une ou plusieurs machine. Par exemple: scanner une plage d'adresse IP sur le port 21 pour trouver des FTPs.

Flooders : La plupart des boards disposent d'un anti-flooding, c'est à dire une routine évitant à une même personne de faire trop de replys à la suite, par exemple vous ne pourrez faire un reply que toutes les 30 s...
Un flooder est donc celui qui reply à gogo avec très peu de corps dans le message, genre 'mdr' ou 'thanks' . En général les propriétaires des posts à qui vous répondez aiment bien (et j'en fais parti...) un petit message sympa plutôt que 1 mot !

Leecheurs : Alors là attention ! Le leecheur n'est pas un personnage sympathique ! Il s'agit de celui qui écume les boards, qui mate toutes les IP et qui ne fait aucun reply. Le problème c'est qu'il y a beaucoup trop de leecheurs, il n'y a qu'à regarder les stats des boards...
Alors s'il vous plaît les amis, n'oubliez pas qu'un petit reply fait toujours plaisir !

Deleters : Nous atteignons ici le sommum du chacal , voire du coyotte qui fréquente les boards ! Le deleter est un leecheur ultime, car non content de mater les IP de vos posts, il s'y rend, pompe tout ce que vous avez mis si longtemps à upper, et content de lui

efface tranquillement tous les dossiers...Une sale vermine je vous le disais !
Pour s'en prémunir plusieurs solutions s'offrent à vous que nous verrons plus tard.

TAGS : Tags, comme en français ça représente un tag, on parle là de l'indication qu'un Pub est déjà utilisé par quelqu'un. En général c'est un dossier de type ".temp", ".tagged", "~tmp" et de nombreux autres que vous trouverez par expérience.

TAGGER : "tagger" signifie créer des répertoires dans le ftp pour y inscrire différentes informations comme le nom de l'uploader, le nom du scanneur, le nom du taggeur, le nom de la team pour qui vous avez uploader ainsi que le non de la release mais cela sert aussi à cacher vos fichiers uploader dans le ftp pour pas que les autres scanneurs ou le sysop ne les voient mais nous verrons ça plus tard.

UPLOADER : c'est à dire envoyer des fichiers au ftp on dit également upper ou up.

DOWNLOADER : c'est à dire télécharger des fichiers du ftp on dit aussi dl.

FAI : c'est votre fournisseur accès a internet en un mot c'est par lui que transite vos communications.

T1,T2,T3 : Ce sont des lignes louées qui permettent la transmission de données à moyens et hauts débits (2,4 Kbps à 140 Mbps) en liaison point à point ou multipoints (service Transfix).
Les 3 lignes les plus répandues sont les T1 (1.5Mbps), les T2 (6 Mbps), et les T3 (45Mbps). Il existe aussi des lignes nettement plus rapides: ce sont les E1 (2Mbps), E2 (8Mbps), E3 (34Mbps), et E4 (140Mbps) qui sont inaccessibles pour les particuliers.

SYSOP : Sysop est le diminutif de Système Opérator. C'est la personne qui est sensée gérer, administrer et surveiller les serveurs pub (FTP pour nous). Il a tous les droits comme effacer des fichiers, couper les accès anonyme ou bien même fermer le serveur.donc la personne à éviter car s' il tombe sur votre up il l'effacera tout simplement et fermera peut-être l'accès anonymous du ftp.

FXP : fxp signifie "File Exchange Protocol". Sert pour échanger des fichiers entre deux serveurs on dit alors qu'il est fxpable c'est à dire qu'il peut uploader ou downloader des fichiers sur un autre serveur mais nous verrons ça en détail plus tard.

DUMP : Serveur Principal qu'on ne post jamais, il sert à stocker tous les fichiers que l'on transfert vers divers Pubs. Un DUMP est généralement un serveur Unix FXPable, les très bons DUMP (ceux qui sont très rapides et possèdent beaucoup d'espace libre sont très rares, donc très durs à trouver). Les DUMPs sont les outils les plus précieux pour FXP. Il est conseillé de retourner à la racine, de temps à autre, pour surveiller que personne d'autre ne vient s'installer, car s'il post votre DUMP sur un forum le Sysop risque de détecter un afflux anormal de connections et d'en chercher l'origine, et par conséquent de trouver et d'effacer votre dossier.
Si quelqu'un s'installe, ne vous énervez pas, n'effacez rien, contentez-vous de poster un message dans chaque dossier indiquant que vous utilisez actuellement ce serveur, et attendez de voir comment réagit l'autre personne.il est maintenant tres courant de voir des dumps sur des serveurs privés(Serv-U, G6....) accessibles uniquement aux personnes authorisées.

Port : Lors d'une connexion à un ordinateur hôte, il est nécessaire de spécifier l'adresse de cet hôte mais aussi son port. Le numéro de port va spécifier le type de communication que vous allez avoir avec cet hôte. Par exemple, le port pour une communication Telnet est 23, celle pour une communication HTTP est 80 et celle pour le ftp est le 21. Le port TCP est codé sur 16 bits.

DNS : (Domain Name Service): Ce terme a plusieurs significations : c'est le protocole par lequel on peut obtenir l'adresse IP d'une machine dont on connaît le nom. Ce nom est aussi appelé DNS. Enfin, les serveurs implémentant ce protocole sont aussi appelés DNS pour Domain Name Server.

Proxy : Machine servant de tampon entre un client et un serveur cible. Il retransmet les données envoyées par le client et les envoient au serveur cible. Certains proxy sont anonymes (il ne donne pas l'adresse du client au serveur) certains sont transparent(le serveur cible croit que le proxy est le vrai client), certains sont chaînable (on peut les mettre les un à la suite des autres pour être sûr que le serveur cible aient des difficultés à retrouver le client). Il peut être en écoute sur port 80, 8080, 3128... Certains acceptent de passer autre chose que des commandes HTTP(web) comme du FTP ou autre...(nous verons ca plus tard)

Wingate : C'est un proxy propriétaire qui fonctionne sur les ports correspondant a l'application: par exemple pour faire du FTP en passant par une wingate, il faut se connecter sur son port 21.

2. COMMENT SCANNER DES FTPS :

Savoir de quoi on parle ...

Le scanning commence bien sûr par savoir ce que l'on scanne. Une adresse IP est de la forme xxx.xxx.xxx.xxx, 4 chiffre dont la valeur varie de 0 à 255. Une ip c'est un numéro de ce style là 193.252.19.154 (de 0.0.0.0 à 255.255.255.255) qui sert à identifier tous les ordinateurs (pc/mac etc..) connectés au réseau mondial "internet", un peu comme un numéro de téléphone. La plus grosse ip est 255.255.255.255 et la plus petite est 1.1.1.1 mais elles ne correspondent à rien. Par exemple pour connaître l'IP de votre ordinateur attribuer par votre fai, lancez une invite de commande Ms-dos et faite "winipcfg" si vous êtes sur win98 ou "ipconfig" si vous êtes sous win 2000. Pour ce qui nous concerne il faut rechercher des IP sur lesquelles on pourra se connecter pour uploader des fichiers . Cela s'appelle "scanné" des IP .

Nous avons vu que l'ensemble des IP sur le net va donc de 0.0.0.0 à 255.255.255.255 ce qui donne un nombre total d'IP de 256 puissance 4 : 4.294.967.296 adresses (malgré ce chiffre, tout le net a dû être scanné au moins 100 fois).Une adresse IP est donc un nombre codé sur 32bits (4 paquet de 8 bits = 4 paquets de 1 octet)

Ces adresses sont réparties en 5 classes:

Classe A

La classe A va de : 0.0.0.0 à 127.255.255.255

Le premier octet de l'IP sert à l'identification d'1 seul réseau.
(64.xxx.xxx.xxx par exemple)
1 réseau de classe A comprend donc 16.777.216 serveurs possibles.
Cette classe est réservée aux très grosses organisations du type de celles qui gèrent internet, les armées, etc...
Cependant aussi grosse soit l'organisation , aucune d'entre elles n'utilise toutes les adresses de son réseau , TRES loin de là (de l'ordre de 0.01% de serveurs utilisés sauf dans certains cas très spéciaux)

Classe B

La classe B va de : 128.0.0.0 à 191.255.255.255

Les 2 premiers octets de l'IP servent à l'identification d'1 réseau.
(158.78.xxx.xxx par exemple)
1 réseau de classe B comprend donc 65.536 serveurs possibles.
Ce type d'adresse est attribué à certaines organisations moins importantes et à de très grosses entreprises, mais surtout à des universités. (important pour ce qui nous intéresse on verra pourquoi plus loin)
Encore une fois, aucune organisation ou entreprise n'utilise autant de serveurs (de l'ordre de 1 à 2%)

Classe C

La classe C va de : 192.0.0.0 à 223.255.255.255

Les 3 premiers octets de l'IP servent à l'identification d'1 réseau.
(198.65.128.xxx par exemple)
1 réseau de classe C comprend donc 256 serveurs possibles.
Ce type d'adresse est attribué à de petites organisations, des serveurs web, bref ce sont les plus courantes.
Et là, il arrive qu'un réseau utilise la totalité de ses serveurs, voire s'étende sur plusieurs plages d'adresses consécutives.

Classe D

LA classe D va de: 224.0.0.0 à 239.255.255.255

Les adresses de cette classe limitent théoriquement la taille d'un réseau à 1 seule adresse IP.
En réalité, il s'agit d'adresses utilisées pour la diffusion restreinte encore appelée mutli-diffusion; elles permettent de remettre un paquet à un ensemble d'ordinateurs. En clair plusieurs ordinateurs partagent une seule adresse (bref, vous ne risquez pas de trouver un pub dans ces adresses...).

Classe E

La classe E va de: 240.0.0.0 à 255.255.255.255

Ces adresses sont réservées à un usage ultérieur de l'internet (en clair, n'espérez pas y trouver quelque chose si vous trouvez kelke chose la , je vous paie le champagne et une pute)
Voilà qui a dû vous aider à comprendre la structure du net. Vous devriez avoir une vision un peu plus précise de l'internet et vous devriez même voir où se trouvent les bons ranges.

En clair comme vous l'avez compris, les classes D et E sont à oublier d'office (sauf si vous voulez scanner dans le vide cybernétique du net). Il nous reste les classes A ,B et C

- le plus simple (et ce que je conseille toujours pour un premier scan) c'est les adresses de classe C. Pourquoi? Parce que c la que

vous trouverez le plus grand nombre de serveurs (pas difficile a deviner puisque les réseaux sont moins grands -> ils sont plus nombreux ou plus "serrés" sur les ranges d'IP pour donner une image.) Mais maintenant , réfléchissont un peu... La plupart des IP de la classe C appartiennent a des serveurs web (95%).En clair , en scannant sur ces ranges d'IP , la plupart des pubs que vous trouverez seront des support FTP de site HTTP et c clair que mis a part sur de GROS site la vitesse ne sera pas des meilleures (entre 50ko/s et 500 ko/s) et l'espace sera restreint (rarement + de 2 Go libres)

- Cependant, pour trouver des pubs plus rapides, il vaut mieux scanner la classe B et plus précisément les universités. Pourquoi? Parce qu'elles ont une très grosse bande passante et beaucoup de serveurs dédiés aux besoins éducatifs. En général, soit c'est une très grosse bande passante (type T3 ou OC-3) partagée entre tous les serveurs, soit c'est plusieurs bandes passantes moins grosse (type T1) allouées chacune à un groupe de serveurs.
Attention cependant, ne croyez pas que parce que vous allez scanner de l'université que vous aurez tous vos pub avec une vitesse minimale de 1 mo/s. C'EST FAUX pasque beaucoup de serveurs sont limités avec une bande pssante alloué par serveur (genre 100 ko/s pour 1 serveur) Néanmoins , vous aurez beaucoup moins de résultats qu'en scannant de la Classe C mais ces résultats seront de meilleure qualité le plus souvent.

- quand a scanner de la classe A.....Si vous avez envie de laisser tourner un scan plusieurs jours pour quelques résultats c'est votre probleme. mais on peux avoir de très bonnes surprises parfois Donc , voila , maintenant , vous devriez pouvoir faire un choix sur koi scanner, vous savez ou vous allez .

encore une chose les ftps commence souvent par : 64 , 205 j'usqu a 216 enfin voila les ips le + souvent scanner

206.xxx.xxx.xxx,
207.xxx.xxx.xxx,
208.xxx.xxx.xxx,
209.xxx.xxx.xxx,
216.xxx.xxx.xxx.
Mais les adresses suivantes ont aussi de bonnes chance d'être de bons futurs pubs :
204.xxx.xxx.xxx à 209.xxx.xxx.xxx,
Vous pouvez aussi tentez d'utilisez les sites des universités par exemple pour celles des USA :
128.xxx.xxx.xxx à 135.xxx.xxx.xxx.

La plupart des universités, IUT etc ont des connections rapides pour le net pour leurs recherches et apprentissages. Ces en général des IP de Classe B (128 à 191) (voire de 30 à 40 pour les vielles facs us donc une Classe A généralement plus rapide), donc chercher l'adresse de celles que vous connessez du genre www.mafac.edu. Cela peut donner de bons résultats.
Je ne vous cacherez pas que le filon est plus que connu et utilisé pour notre plus grande joie car les facs ont souvent leur servers permettant souvent l'utilisation de client FXP héhé le paradis sur terre quoi.
Voila d'autre "bonnes adresses" :
63.xxx.xxx.xxx
35.xxx.xxx.xxx
4.xxx.xxx.xxx

il y a des categories d'ip en plus qu'il est complétement innutile de scanner... c'est les ip privées ! Car dans toute la description on parle que d'ip publiques. Les adresses privées ce sont celle qui ne sont pas autorisées à circuler sur le web... donc cela ne sert à rien de chercher à les scanner.... il y en a une plage par classe. Donc 1 pour les classes A : 10.0.0.0 - 10.255.255.255, 16 pour les classes B : 172.16.0.0 - 172.31.255.255 et 255 pour les classes C : 192.168.0.0 -192.168.255.255 tout le monde les utilisent dans les sociétés qui ne communiquent avec internet qu'à travers un routeur. bon on va pas non plus s'etendre dans les détails...

3. Le scanning en lui-meme :

Bon bah voila un ptit tutorial assez simple sur le scan, n'hesitez pas a commenter, je vous propose pas LA solution mais UNE solution et toute critique sera la bienvenue...
Tout d'abord il faut 3 chose :

Un PC
Un acces au net
Un logiciel de scan : Grim's Ping (C'est pas le plus rapide, mais le plus simple c'est sur), vous trouverez Grim's Ping à l'adresse suivante : http://grimsping.cjb.net/

Qu'est-ce que le scanning?

C'est un processus qui consiste à envoyer des requêtes FTP (connexion sur le port 21) et à tester si l'IP ciblée répond à une connexion anonyme.

En clair, le logiciel de scan envoie la requête:
- Si l'IP ne répond pas (pas de machine à cette adresse ou pas de serveur FTP) : le logiciel passe à l'IP suivante
- Si la machine répond : le logiciel teste l'accès anonyme

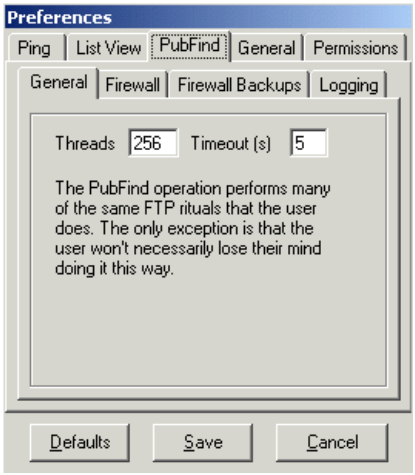
- Si l'accès anonyme est permis, il cherche des répertoire avec permission d'écriture
- Si il n'en trouve pas, il passe à l'IP suivante
- Si il trouve, bien joué, vous avez trouvé un pub

Pourquoi Grim's Ping ?

Donc ce soft, sert à scanner des plages IP, par ex. de xxx.xxx.206.0 à xxx.xxx.206.255.
De plus grâce a sont système de queue list, vous permettra de scanner plusieurs ranges facilement et dans lancer une bonne grosse liste pour la nuit ;-).

Vous me direz, jusque là, rien de spécial, mais là ou Grim's Ping arrive à se demarquer de ses concurrents (omega, PH, ftpscanner...) c'est qu'il peut, aussi bien vérifier les droits d'écriture sur des répertoires donnés (/pub, /incoming, ...), que de vérifier si le ftp est FXPable. Et en plus réalise un test de vitesse, détecte l'OS (W2k, Linux,...) et même des fois la config du serveur (P4 bi-proc..2Ghz ;-))! Mais tout ceci vous pourrez choisir de le faire tester ou pas car évidement çà ralenti ...
Donc vous l'aurez compris, Grim's Ping est la Rolls Royce du scan !

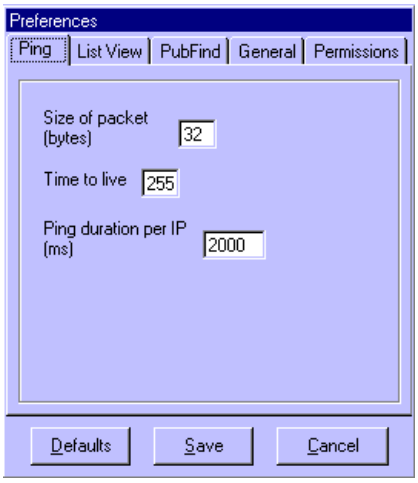
Configuration de Grim's Ping



Passons à la partie pratique. Apres l'installation, la premier chose à faire est de configurer Grim's Ping
Ouvrir Grim's Ping puis taper "F8" pour entrer dans les options.
Onglet "PubFind" =>"general".
Dans "Threads" ,configurez selon votre connexion:

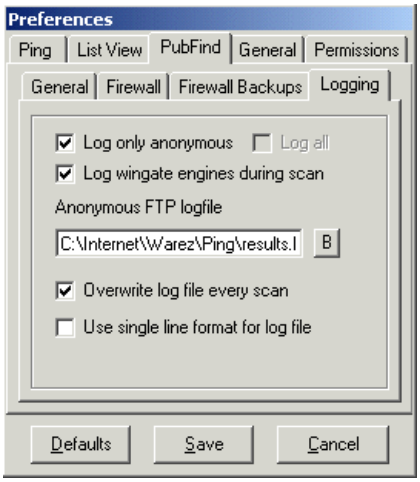
Connection Tel.- 56k 40
ISDN - 64k - 128k 80
ADSL / Cable - 512k -1Mo 190
T1 ou plus - 1Mo +++ 350

Evidement si vous surfez ou DL en même temps mieux vaux réduire la cadence ;-)
Dans "Timeout" (temps d'attente de réponse du serveur.) mettez y "5" comme cela le seveur, si vous en trouvez un, sera rapide ;-)
en fait, 200 signifie que Grim's Ping va verifier 200 ips en même temps

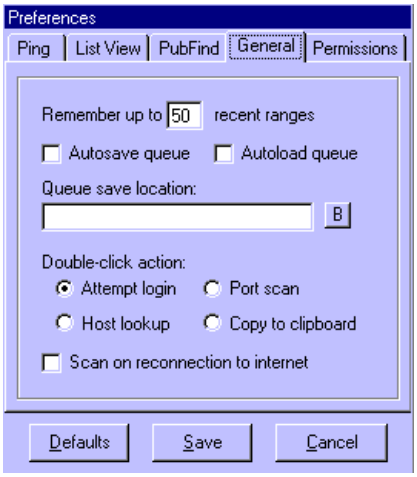


Allez dans Options : Preferences : Onglet Ping

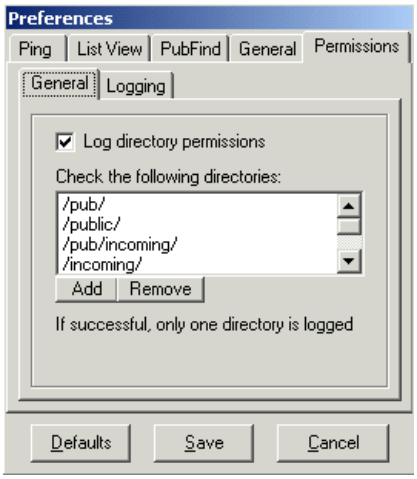
Size of packet (bytes): 32
Time to live: 255
Ping duration per IP (ms): 2000



Onglet "PubFind" => "Logging" .
Cochez "log only anonym" et "log wingate".
La première option sert à garder tous les ftps loggés et la seconde les wingate.
Les informations sont stockés dans un fichier txt accessible par "F3" dans l'interface
décochez tout le reste et choisissez le path de votre results.log.



Allez dans Options : Preferences : Onglet General
Remember up to 50 recent ranges
Décochez tout le reste, choisissez le path de votre queue.txt



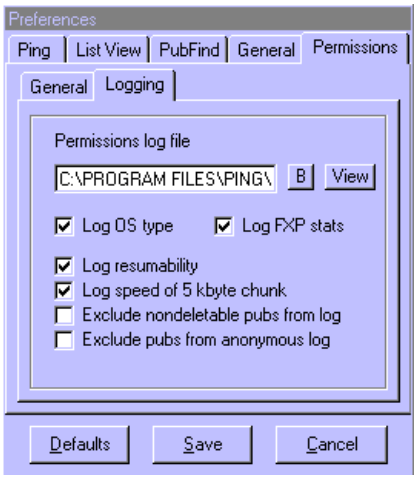
Autres chose à faire est d'ajouter cette liste de repertoire dans la liste des répertoires à tester pour les permissions d'ecriture:

Onglet "Permissions" > "General"
C'est l'option qui permet de faire verifier l'écriture sur les ftps.

Cochez "log directory..."
Dans "check the following directories" pour avoir plus de chance de trouver les rép avec les droits d'ecriture, Enlevez tous les répertoires existants et rajoutez ceux-ci:

/
/_vti_pvt/
/upload/
/home/
/public/
/pub/
/temp/
/wwwroot/
/cgi-bin/
/cgibin/
/incoming/
/in/
/_vti_cnf/
/_vti_txt/
/_vti_log/
/anonymous/
/outgoing/
/tmp/
/mailroot/
/ftproot/
/images/
/_private/
/usr/
/pub/incoming/
/public/incoming/
/anonymous/_vti_pvt/
/anonymous/incoming/
/anonymous/pub/
/anonymous/public/
/usr/incoming/

Veillez à bien respecter l'ordre. En effet, au fur et à mesure de mes scans, j'ai défini cet ordre particulier pour les cas les plus courants car Grim vérifie les permissions d'écriture une à une et les placer ainsi fait gagner un temps non négligeable sur un gros scan.



dans l'onglet Logging, cochez "Log OS type", "Log FXP stats", "Log resumability" et "Log speed of 5 kbyte chunk". Assurez vous que "Exclude nondeletable pubs from log" et " Exclude pubs fromanonymous log sont décoché et choisissez le path de vos futurs perms.log.

NOTE SUR LES PROXYS :

Beaucoup s'inquiètent au sujet de l'illégalité du scanning et le fait qu'ils pourraient predre leur connexion. Personnellement je n'utilise pas de proxy (pour ceux qui ne savent pas ce que c'est, en passant par un proxy qui est une machine comme une autre, vous lui dites de scanner telles IPs et lui vous renvoie les résultats, ce qui procure un anonymat relatif), et ce pour deux raisons:
- La première est que c'est beaucoup mois rapide, n'espérez pas dépasser 20-30 threads en passant par un proxy.
- La seconde, que les sysops (admins des ftps) ont autre chose à foutre que de faire de la délation auprès de votre FAI pasque

vous êtes le 458ème méchant de la journée à scanner leurs machines, d'autant plsu si vous n'avez pas la même nationalité (Pour cela je déconseille quand même le scan sur votre territoire).

De plus, un préavis doit vous être envoyé par votre FAI avant toute sanction et si cela devait arriver, et bien, well, it's life you see, tout n'est pas rose mon bonhomme, chacun prend des risques dans le monde du warez

Qu'est ce que c est un proxy???? (definition exacte)

Ba un proxy en faite c est un serveur comme les serveur ou on tagg)))) Donc si vous utiliser un proxy la premiere chose qui se passe c' est que vous vous y connecter et apres tout ce que vous faite passe par ce proxy, donc a l' arriver (sur le serveur de wanadoo par exmple))) cest pas votre ip qui aparait mais celle du serveur proxy, donc pour vous retrouver ca va etre dure, surtout qu il y a des proxy anonyme.

Je tiens aussi a preciser que si vous "interneter" a l etranger y a pas trop de risque que le mec se prenne la tete a nous retrouver.....Donc les proxy sont surtout a utiliser si on est sur un serveur francais.... Les proxy peuvent ralentir votre connexion (si il sont lents) masi peuvent aussi l ameliorer legerement (si vous trouver de bon proxy poster le ici sur le board pour en faire profiter toute la team merci...).

A-Les types de proxy:

1-Les proxy dit normal
Ils ne servent que pour le surf (ou presque on verras ca plus bas)

2-Les socks
Ils nous permettent de tout faire icq, ftp, http , mail en passant par lui....

Vous pouvez choisir un proxy sur une liste et le parametrer manuelement ds votre logiciel ftp ou navigateur...ce procede est long (si vous trouver pas un bon proxy tout de suite) le mieux c est d utiliser des logiciels specialise...

B-Les Logiciels...

1-Socks Caps
Ca c est le top.... c est un petit logiciel simple d install.. et vous n avez pas a parametrer vos programmes.. le seul truc c est qu il faut lancer vos progrmamme (ftp, navigateur) directement a partir de Socks Caps.. mais il vous permet de tout faire icq, ftp etc....il utilise des socket 5 les meilleurs mais dure a trouver ..

logiciel: http://www.socks.nec.com/

2-HTTPORT
Permet d utiliser des proxy normal pour le ftp , icq etc.. donc transforme un proxy normal en sock 5 en quelque sorte.....
il faut parametrer les logiciels

logiciel: http://www.htthost.com/

3-Multiproxy
ca c est le top aussi.. mais je sais pas si on peut utiliser les socks mais je pense que oui...il faut parametrer les logiciels..
Il permet de changer de proxy automatiquement, a chaque requete (sequentiellement ou aleatoirement).
Une liste de proxies est disponible sur le site web, "mise a jour" regulierement. (Mais vous pouvez bien sur ajouter d'autres proxies).
Il teste aussi une liste de proxy (a partir d un txt) on pourras ainsi voir les plus rapides.....
TRES BON LOGICIEL si il accepte les socks bien sure...

doc et logiciel: http://www.multiproxy.org/

4-Anonymity 4 Proxy
A partir de listes de Proxies, le logiciel va les tester, et vous pourrez les utiliser sans modifier les parametrages de vos autres logiciels
.. il a l air pas mal du tout....
site officiel: http://www.inetprivacy.com/ anglais

On peut aussi telecharger ces logiciels sur les site les plus connu http://www.telecharger.com
zdnet http://www.download.com
etc...

5-les wingates

Une autre façon de cacher votre identité est de transférer vos fichiers au travers d'une Wingate. Wingate est installé sur un ordinateur Win 9x/NT et est utilisé comme serveur pour un LAN. Tous les Pc connectés à ce réseau accéderons à Internet au travers de cette Wingate. Wingate fonctionne un peu différemment des proxy socks. Si vous vous loguez sur 2 sites sur le même port, les fichiers que vous allez transférer vont passer par la wingate. L'avantage est que cela vous permet de FXP des fichiers vers des sites que vous n'auriez pu FXP avant. L'inconvénient est que la vitesse du transfert est limitée par la vitesse de la Wingate que vous utilisez. Les Wingates son généralement très occupées et donc très lente. A moins que vous ne puissiez absolument pas FXP entre 2 sites vous n'utiliserez pas Wingate car cela ralentirais votre transfert 99,99% des fois… Wingate offre de nombreux services mais soyez surs que vous transférez les fichiers par le port 21 et non le port 23 ! les wingates se trouve aussi en scannant des plage ip sous Grim's Ping il suffit pour cela a la fin d'un scan d'appuyer sur la touche F3 et si vous en avait trouvée devant certaine adresse vous drevrier voire WinGate engine s'afficher. La wingate est pratique car elle permet de transférer des données même entre 2 FTPs non FXPable. Et ca c'est le top. Seulement voila c'est dur à trouver et c'est pas très rapide.

Le plus simple c'est d'installer Multiproxy juste pour tester les proxy (vous télécharger la liste des socks voir la liste des serveur exotique ou y a des sock..), donc après les avoir tester vous choisissez le plus rapide...
après vous lancer votre logiciel ftp et vous lui dite d'utiliser ce proxy..... et voila c'est bon votre ip n'apparaît plus .. pareil pour votre navigateur.. c est super rapide et efficace le plus dure c est d ajouter vos proxy dans la liste de Multiproxy (effacer la liste qui y est déjà car ce ne sont pas des socks...) pareil pour votre navigateur si vous voulez cacher votre adresse quand vous surfer...

RESULTAT FINAL DES TESTS

POUR scan,navig etc.....
bon comme je l'ais dit suffit de trouver un proxy (qui accepte le port 23 pour le scan) y en a plein

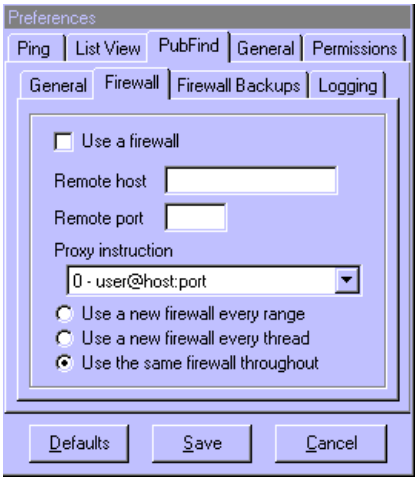
-POUR LE FTP
il n y a que les sock qui fonctionne, pas les proxy , ni les proxy qui supporte le mode sock port 1080 (les proxy connect)
Les socks c est ceut qui on le port 1080 par defaut
Donc après vous aller dans les paramètre de votre ftp et vous le mettez...

-pour le fxp
pour le fxp utiliser une wingate de préférence si vous en avait des rapides.
Bin disons que pour les gros fichier que l'on veux mirrorer un peu partout, mieux vaut utiliser un Socks et un FTP FXPable alors que si on fait un transfert de petits fichiers, la wingate peut être + intéressante (à condition d'en trouver une + rapide supérieur a 10 Ko/s

De toutes façons, quelque soit la vitesse du proxy, elle n'influera pas sur la vitesse du transfert inter serveur.
Le Proxy sert uniquement dans notre cas à transférer les commandes que l'ont donnent aux FTPs.
Le serveur final ne connaît pas le client initial: Pour lui c'est le proxy qui envoie les commandes. Par contre, ne pas oublier que comme n'importe quel serveur, le proxy garde une log des connexions....
D'où l'importance d'utiliser 2 proxys différents pour les 2 FTPs sur lesquels on se connecte, ainsi, même si les serveurs qui reçoivent les données peuvent se contacter (en regardant leur log) ils auront beaucoup de mal à retrouver l'initiateur des commandes.

Grim's Ping permet aussi de scanner avec un proxy. Pour cela il faut que tu trouves un proxy qui accepte le FTP. en allant chercher sur des sites recensant les proxy. Personnellement, je n'utilise pas de proxy car la plupart du temps il accepte une seule connections a la fois (a moins de trouver un bon proxy wingate ou winproxy ou tu peux monter jusqu'a 20 ou 30 threads, tu peut en trouver sur Internet). Ce qui rallonge le temps du scannage de 255 fois (pour 100 ip scanner, sans proxy il mettra 8 sec, avec un proxy pour 1 treads, il mettra environs 13 min. Tu vois la différence.). Le risque de scanner sans proxy et que ton provider reçoive un mail de la société que tu scannes annonçant qu'il y a eu tentative d'intrusion illégale. Tu recevras des avertissements et au pire on fermera ton compte. Tu peux changer de provider. J'ai scanne pas mal de temps et j'attends toujours les avertissements de mon provider. Une autre chose, il y a quelques ip a éviter de scanner notamment les ip de l'armées ou du gouvernement .gov et .mil (gouvernement et militaire) sauf si vous étés kamikaze. Ainsi que ton fai ou tout autres fai d'ailleurs. ne scanner pas les site de la NASA et du FBI les ip françaises vous devinez pourquoi. maintenant pour savoir qui vous scanner vous pouvait télécharger samspade sur www.samspade.org. Le mieux pour éviter tous problème étant de trouver des ip d'universités a l'étrangers.

Voila c'est la fin de de la note sur les proxys vous pouvez donc scanner et faire du ftp en toute sécurité, Juste un dernier mot pour l'épilogue si vous voulez Toutefois utilisez un proxy je vous donne la manipulation a effectuer pour configurer Grim's Ping correctement.



Onglet "PubFind" => "firewall" .
Si vous souhaitez utiliser un proxy/firewall.
Port 1080 pour les proxy sock 4/5 et 23 pour les wingate.
Bon çà ce trouve où des proxys me direz vous ! ...et bien ici http://tools.rosinstrument.com/proxy/socks.htm
Ou http://www.cyberarmy.com/lists/proxy/

En faite pour les scans ca marche du tonnerre.. pour le ftp toujours pas trouver de super (mais me suis pas prit la tête a chercher)...

Car le plus dangereux étant de scanner et non pas de downloader ou uploader

Pour vérifier votre anonymat allez voir ici, si c'est votre IP qui est transférer: http://www.all-nettools.com/pr.htm

Bon ca y est, Grim's Ping est configuré, reste à trouver des ip pour commencer. Je vous conseille de scanner des plages d'ip en commencent par les université étrangères, vous trouverez assez facilement des pubs. Pour récupérer les url d'universités étrangères c'est ici http://www.agora.stm.it/university/uni.htm . Y a de quoi faire ici...

Une fois l'url récupérée, vous allez dans la barre des taches : demarrer - executer - et vs tapez "command" ca va vs ouvrir une fenetre MS-Dos. Vous tapez ensuite ping suivi de l'url.
Exemple:

C:\Ping http://www.yahoo.com
Envoi d'une requête 'ping' sur http://www.yahoo.akadns.net [64.58.76.178] avec 32 octets de données :

Réponse de 64.58.76.178 : octets=32 temps=138 ms TTL=240
Réponse de 64.58.76.178 : octets=32 temps=151 ms TTL=240
Réponse de 64.58.76.178 : octets=32 temps=137 ms TTL=240
Réponse de 64.58.76.178 : octets=32 temps=124 ms TTL=240

Statistiques Ping pour 64.58.76.178:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en milli-secondes :
minimum = 124ms, maximum = 151ms, moyenne = 137ms

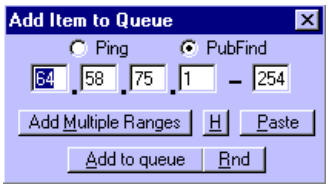
et la bien sur vs recupérez l'ip ici c'est 64.58.76.178...

Autre méthode :
il suffit de faire F9 ou menu tools single host lookup dans grim's ping,une petite fenetre s'ouvre il suffit de coller l'url et il te donne l'ip directement

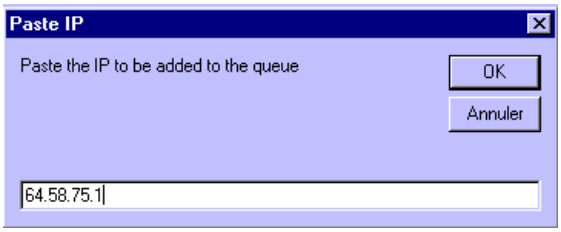
Pour avoir une idée encore plus précise de savoir quoi scanner, allez faire un tour sur www.ipindex.net/

Ce site répertorie et identifie les réseaux des classes A, B et C souvent mise a jours.

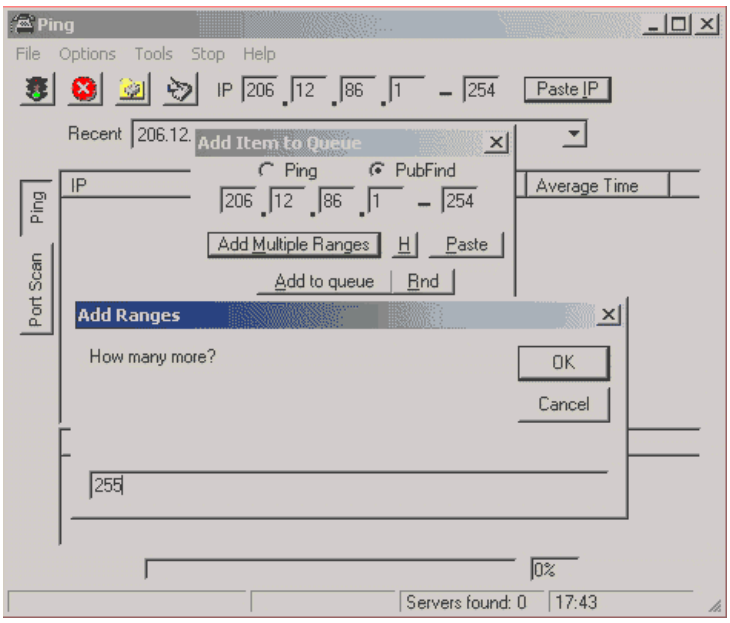
Sachant que le scanning est illégal, veillez quand même à éviter tout ce qui est français (on est jamais à l'abri d'un coup de pute de la part de son FAI...).



Une fois l'ip choisi vous retournez sous grim's ping et cliquez sur 'add new entry" (touche F6) vous cochez la case "PubFind" et vous rentrez l'ip que vous avez choisi moins une plage, ici l'ip etait 64.58.76.178, je mets donc 64.58.75.1 (vous commencer le scan a 1).



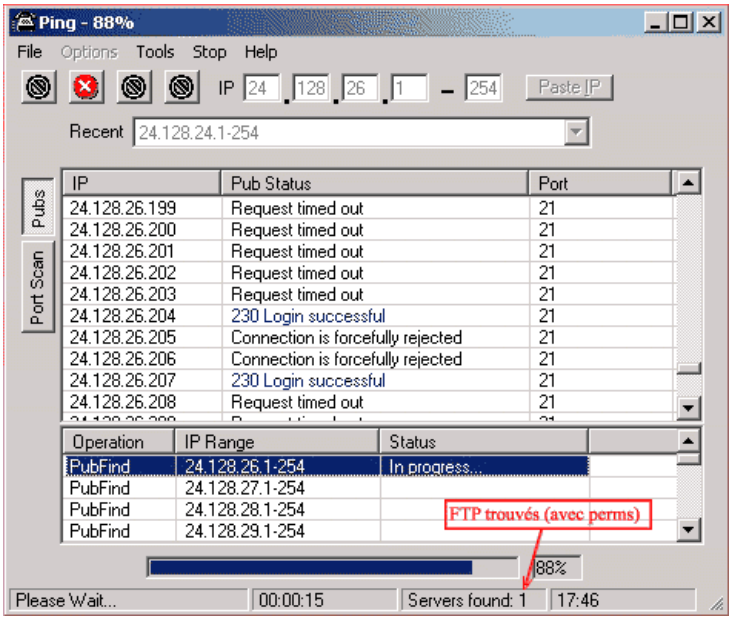
vous pouvez directement entrer l'ip en appuyant sur past la fenêtre s'ouvre et il n'y a plus qu'a rentrer l'ip comme ceci 64.58.75.1 et ensuite d'appuyer sur entrer.



-Cliquez sur add to queue pour scanner une seule série par exemple (206.12.86.0 à 206.12.86.255)
ou
-Cliquez sur Add multiple ranges pour scanner plusieurs séries d' IPs:
206.12.86.1 à 206.12.86.255
206.12.87.1 à 206.12.87.255
206.12.88.1 à 206.12.88.255

(dans ce cas une seconde fenêtre s'ouvre pour savoir combien de série vous voulez mettre en queue
255 dans cet exemple au minimum si vous voulez trouver des pubs sur.)

Vous fermez la fenêtre et cliquer sur "go" (le petit feu vert) ou appuyer sur la touche F5... Et vous attendez...
Vous devez voir ceci ci tous c'est bien passer



Une fois le scan finis, il va vous indiquer en bas a droite le nombre de pub trouvé il vous reste plus qu'a les éditer (touche F2).

Note : si vous trouver des pub avec des ip très proche comme par exemple 24.128.26.201 24.128.26.202 24.128.26.203 il y a de forte change pour qu'il s'agis du même serveur tester et si il s'avère que ce soit le même serveur pas la peine de poster trois fois le même faite votre choix et poster en un.

encore une autre méthode,

Explications pratiques :

Lorsque j'ai trouvé une bonne range d'IP, voilà comment je procède:

1ère étape:

Dans Grim's Ping, cliquez sur "Paste IP" et rentrer le début de votre range (par exemple 127.24.0.0). Là vous verrez la fenêtre "Add Item to Queue" s'afficher avec 127.24.0.1-254, si le 254 n'apparaît pas, mettez le. Cochez "Ping" puis cliquez sur "Add Multiple Ranges" et entrez le nombre de ranges que vous voulez faire, par exemple, si vous rentrez 10, il scannera de 127.24.0.0 à 127.24.10.255. Comme je fais tourner souvent la nuit, je rentre 6000 puis j'arrête le tout en me levant le lendemain, c'est brutal mais efficace

Faites attention à la configuration de votre FireWall si vous en avez un, il ne faut pas qu'il bloque Grim's Ping.

Fermez la fenêtre "Add Item to Queue" puis lancez le scan en cliquant sur le feu vert. C'est parti!!!

(Je ne m'attarderai pas sur les messages du PubStatus pendant le scan, vous aurez certainement mieux à faire que de regarder Grim's Ping mouliner comme un malade...)

2nde étape:

Une fois la première passe de scan terminée ou que vous en avez marre et que vous avez stoppé le processus, dans le path que vous avez indiqué précédemment dans les options, vous trouverez un joli fichier results.log contenant la liste des ftps accessibles en anonyme sur les ranges d'IP scannées. Si tel n'est pas le cas, ça merdouille du côté de votre FireWall ou des options de Grim, ou alors vous avez scanné dans le vent (on est pas assuré de trouver ne serait-ce qu'un ftp sur une range).

Bon si tout s'est bien passé, votre results.log est rempli, vous le sauvegarder dans un autre répertoire et on passe à la deuxième passe de scan:

Dans la fenêtre de status du bas, là où les ranges à scanner s'affichent, faites un clic droit et choisissez Queue list : Import PubFind!. Vous lui indiquez le chemin où se trouve votre results.log. Voilà donc tous les ftps anonymes sont affichés dans le status. Maintenant, très important, allez dans Options : Préférences : Onglet Permissions : Onglet General et cochez "Log directory permissions". Faites Save et lancez à nouveau le scan.

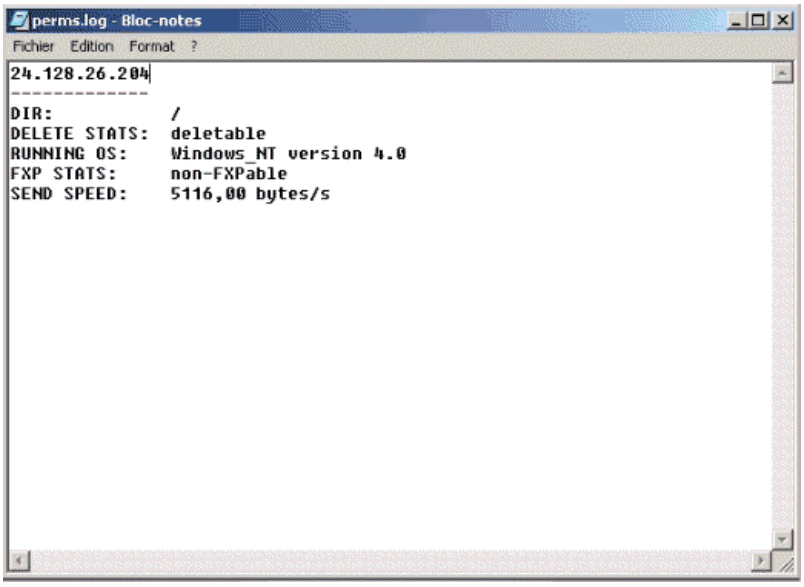
En bas à droite de Grim, vous pourrez observer le compteur "Servers found:" augmenter. Grim logge alors tous les ftps anonymes dans le fichiers perms.log.

Une fois cette deuxième passe assez longue vu qu'il teste tous les répertoires jusqu'à en trouver un avec possibilité d'écriture, vous pouvez fermer Grim et aller voir le contenu de votre perms.log (à sauvegarder aussi).

4. Le test des pubs :

Dans votre fichier perms.log ainsi obtenu a la fin du scan appuez sur F2 pour avoir la liste ou editer le fichier perms.log, vous devriez avoir une présentation comme celle-ci:

Bon si vous avez suivi le tutorial vous devriez avoir une liste d'ip sous cette forme



24.128.26.204

DIR: /pub/incoming/ ----> indique le chemin (le path en anglais) dans lequel vous pouvez uploader
DELETE STATS: nondeletable ----> deletable ou indeletable indique si on peut effacer ou pas les fichiers sur le serveur
RUNNING OS: Windows_NT version 4.0 ----> version du serveur
RESUMABLE: No ----> indique si vous pouvez reprendre un upload ou download qui s est arrêté
FXP STATS: FXPable ----> indique si le serveur est Fxpable ou pas (plus d info)
SEND SPEED: 5125,61 bytes/s ----> vitesse du serveur

Ne le postez surtout pas tel quel sur un board!!! Votre job n'est pas fini!!!

En effet, sur le total de votre fichier perms.log, après tests il ne vous en restera peut-être même pas 20% d'exploitables.

Il vous reste deux grandes étapes et vous pourrez enfin poster le fruit de votre travail: le tagg et enfin le test de FXP.

Test la place disponible sur un pub

Trouver l'espace libre du pub.

C'est possible sur certains serveurs NT (ceux qui supporte la compilation ASP en HTTP)
il suffit d'uploader a la racine du serveur le script space.asp (vous le trouverez en téléchargent l'application ping compagnon sur le site de Grim's Ping) puis vous ouvrez votre navigateur en tapant Http://ip du serveur ftp/space.asp et avec un peu de chance, si cela fonctionne, des informations s'afficheront sur les disques du serveur (Format / espace / OS / Type de DD).Cette manipulation ne fonctionne pas avec les serveur unix.

5. Le tagg de pub :

Cette partie , je la dédie spécialement a tous les scanneurs qui postent leur scans sur les boards de cette façon:

24.128.26.204

DIR: /
DELETE STATS: deletable
RUNNING OS: Windows_NT version 4.0
FXP STATS: non-FXPable
SEND SPEED: 5116.00 bytes/s

c'est a dire exactement de la même façon que Grim's ping leur a donné le résultat :
Et la de suite , j'ai envie de pousser une gueulante a tous ceux qui ne se sont pas fouler OOOOOOOOOHHHHHHHH !!!!! ca y est ca

va mieux j'ai envie de leur dire réveillez vous les mecs bordel, vous croyez que votre travaille ce termine là et moi je dit non.

pourquoi? , parce que pour prendre un exemple , vous avez lancé grim's ping fais un gros scan qui vous a filé 100 résultats , vous êtes heureux . mais dite vous qu'en moyenne 70 à 80 d'entre eux vous seront inutilisables et par mis les survivants seuls 5 à 10 vous permettront de faire un pub de qualité (bonne vitesse et taille).

Tagger c'est quoi ? Bon pour faire une analogie c'est un peu le même principe qu'un vrai tag sur un mur de la ville, c'est a dire une appropriation d'un espace à des fins personnelles et expressives.

Sauf que là, vous allez tagger un ftp , c'est a dire que ca consiste à apposer votre marque et signaler aux autres futurs scanneurs et utilisateurs qui tomberont sur ce pub que cet espace est "réservé" et que vous vous l'êtes "approprié". Cela a toute son importance car ca évite à d'autres uploaders de balancer des fichiers a tort et a travers...

Avant de considérer le cas d'un FTP déjà taggé, voyons comment structurer votre tag:

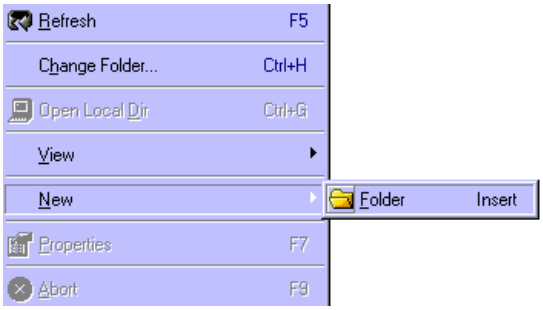
Comment faire ?

Rien de plus simple,il vous faut un client ftp pour vous connecter au ftp il y en a de nombreux mais moi j'utilise SmartFTP qui est le seul client ftp a entrer dans les dossiers "~" ou cachez avec un "." sans connaître le chemin vous le trouverai ici http://www.smartftp.com/. Ensuite il vous faut trouvé une IP valide (cf leçon sur le scan) et non tagguée (j'insiste mais bon...) Pour ça, cherchez les répertoires du style ~tmp, temp, ~temp, .. et tagged pour regarder s'il n'y a pas déja quelqu'un qui ne le se serait "octroyé"., si c'est le cas passer votre chemin si au contraire il n'est pas déjà tagger proceder comme ceci il suffit de créer un nouveau répertoire du style 'tag & scan by titus567' ou 'tagged & scanned par titus567'. Et le tour et jouée ca sera dans ce nouveau répertoire que vous allez uploader par la suite le tagge doit comporte le nom du scanneur et du taggeur en general ce sont les scanneur qui taggue les ftp et les mette a disposition dans la section ftp scanner d'un board

Il doit contenir clairement votre nick et la team pour laquelle vous bossez le cas échéant: (perte de crédibilité WaRnInG)

Si vous avez récupéré une IP d'un ftp deja scanné (de nombreuses board en proposent dans la section scan) , le tag est déjà apposé par le scanneur donc c'est pas la peine d'en rajouter...

Pour tagger avec SmartFTP procéder comme ceci cliquer avec le bouton droit de la souris allez sur new et sur floder cliquer sur le bouton gauche et entrer le nom du répertoire il y a un façon plus rapide c'est d'appuyer sur la touche insert.



6. La protection des taggs :

Pourquoi protéger c'est taggue :

Sachez qu'il est conseillé de créer des chemins d'accès caché pour éviter que le Sysop ne tombe dessus par hasard ou bien que n'importe qui le trouve et efface votre dur travail qui vous a pris des heures et des heures de votre temp. Ca sert également a ce protéger de ces enculer de deleteur .Quoi de plus rageant que de passer plusieurs heures, voir jours sur un Pub, revenir et découvrir qu'au moment où l'on va enfin le poster, tout à disparu …

Pour s'en prémunir plusieurs solutions s'offrent à vous :

- La plus simple est de ne pas montrer l'IP, soit quand le board intègre cette fonction, sinon ne la donner qu'au personnes en faisant la demande sous forme de message privés.

- Trouver des ftp indeletables, mais ce n'est pas toujours facile.

- Cacher les répertoire

- Cree des répertoire labyrinthe

- Cree des dossiers inaccessible

- Les dossiers auto protégés

I Comment Cacher les répertoires :

Il y a plusieurs moyens de cacher un répertoire afin que le sysop du ftp ou les deleters ne les voient pas. Pour cela, il suffit de préfixer le répertoire créer par un caractère spécial ou de créer le répertoire dans un répertoire spécial ...

Alors voilà comment on procède:

Les répertoires préfixer d'un point (.) seront caches sur certains systèmes. Dans la plupart des système Unix, ce type de répertoire sera cachée. Mais parfois, seul le répertoire ".tmp" sera exceptionnellement cache. D'ou la bonne idée de commencer votre structure de répertoire par ce genre de répertoire.

Ex : . /tagged/for/team/xplosion/fxp/ répertoire caché

créer un dossier ayant pour nom Le caractère tilde "~" qui symbolise le 'home directory' complique la tache car lorsque vous envoyez une commande demandant le changement de répertoire vers le répertoire '~', vous serez directement renvoyer vers le 'home directory' de l'utilisateur sur laquelle vous étier loguer. SI vous étés loguer en anonymous, vous vous retrouverez souvent sur la racine du répertoire (ex '/'). C'est pourquoi, lorsque vous double cliquer sur ce genre de répertoire depuis la grande majorité des logiciels client FTP, le ftp affiche les fichiers du répertoire racine. pour accédez à la suite il faut connaître le nom du dossier qui suit et entrer le chemin d'accès dans "Path" , seul SmartFTP les ouvrent (à ma connaissance).
C'est très utilise pour tromper les sysops ou les deleters qui ne reconnaissent pas ce genre de répertoire

Ex : /~/tagged/for/team/xplosion/fxp/ répertoire qui renvoi vers le home directorie

Il est conseillé de mettre des espaces dans les noms (aléatoirement, du genre 2 espaces, 3 espaces, 1 espace …) car certains logiciels ne trouvent pas le chemin s'il contient des espaces.
Ce qui donne des chemins de ce type: /.temp/ tagged/ …

Ex : avant : /~/temp/tagged/for/team/xplosion/fxp / répertoire non caché
apres : / / ~/temp/tagged/for/team/xplosion/fxp / répertoire caché

Pour créer des répertoires cachés, faites une nouveau répertoire comme suit en employant ce format :
/ /dossier1/dossier2

*=espace

Notez bien l'espace entre /*/

L'espace n'est pas un nom mais un ' caractère ' qui n'est pas énuméré, donc rendant les dossiers invisibles au listing.

NOTE: Pour rendre les dossiers cachés, il est préférable de créer plusieurs sous-dossiers avec un espace.

Par exemple : / / / / / / ~/temp/tagged/for / team/xplosion / team/fxp /

Cette technique n'est pas 'anti-suppression', mais permet de rendre un fichier moins accessible en le cachant.

II Comment Cree des repertoires inacessible :

Methode 1 :

Les dossiers inaccessibles empêchent l'utilisateur de parvenir à un dossier. L'utilisateur ne pourra pas entrer dans les répertoires à moins de connaître le chemin des répertoires en entier.

*= espace

1) tu crée un dossier
com1*/*/
2) tjrs à la racine,
com1*/tagged*/*/
3) tjrs à la racine,
com1*/tagged*/by titus567/
4) ben plus qu'à rentrer le path entier, ce qui fait,
com1*/tagged*/by titus567/

ex :

avant : /temp/tagged/for/team/xplosion/fxp /
apres : /com1 /temp / tagged/for/team/xplosion/fxp /

Pour créer des dossiers inaccessibles, employez la liste suivante ' de noms utilisables :
com1 com2 com3 com4 (ports de communication de windows)
lpt1 lpt2 lpt3 lpt4 (ports d'imprimante de windows)

Faites une nouveau répertoire "COM1 / /" par exemple

NOTE: Ceci rend le dossier inaccessible, même à l'administrateur du site., à moins de consulter le DOS(local).

Methode 2 :

Créez un répertoire principal avec le format : prn.hsp.laserjet/ /dossier1/dossier2 etc.

Par exemple : prn.hsp.laserjet/tagged / (note: vous devez créer chaque sous répertoire un par un)

AVANT : /temp/tagged/for/team/xplosion/fxp /
APRES : /prn.hsp.laserjet/temp/tagged/for/team/xplosion/fxp / (bloquez l'accès entier avec le premier dossier)

III Comment Cree des répertoires auto protéger :

Créer un dossier, puis renommer le au format suivant :

dossier1/*./ /dossier2

Cette technique peut s'appliquer aux fichiers en y ajoutant "./ /" à la fin (sans les "") la manip evite que ce soit deleter

Ce qui donne

Fichier movie.rar uppé

Vous renommez le fichier en movie.rar*./*/

*= 1 espace

cela vous fait movie.rar ./ /

Et voilà
Le seul problème de cette astuce est qu'elle ne marche pratiquement que sur des serveur utilisant windows NT 4 ou 5...

Autre petit problème, les admins pourront toujours déléter vos posts, mais c'est plus rare.....

pour les newbies voici un programme pour rendre vos uploade ftp indeletable !! c'est le principe des ././ , mais il fait tout a votre place et donc plus besoins de faire vos fichiers 1 a 1 !! pas cool ça !
le prog s'appele myundelete , et vous pouvez le telecharger ici : www.terra.es/personal6/hi...ete112.zip
pour l'utiliser rien de plus simple , vous lancer le soft et vous donner l'url exacte de votre dossier ! vous cliquer sur make undelete et c'est tout !!! plus facile que ça y a pas

IV Comment Cree des répertoire labyrinthe :

Les répertoires labyrinthes, sont très utile pour se débarrasser des deleters. Si vous créez une arborescence complexe de répertoires factices sur le serveur, celui qui voudra trouver le bon répertoire devra parcourir tous les répertoires factices, s'il n'a pas abandonner avant. Vous poster le bon chemin sur votre board préférés.

Ex : vous crée un répertoire de ce style /temp/tagged & scanned by titus567/for/team/xplosion/fxp /
A la fin vous crée un reptatoire a,b,c,d,e,f,g,h,i,j a l'intérieur du répertoire a vous crée un répertoire 1,2,3,4,5,6,7,8,9 vous refaite la manipulation pour b,c,d,e,f,g,h,i,j vous n'uploader que dans un seul répertoire que vous avait choisie

V La protection Finale

Il s'agit maintenant d'incorporer toutes les techniques en une seule fois

avant : / temp/tagged/for/team/Xplosion/fxp / (aucune protection)
apres : / prn.hsp.laserjet / / /. / /for du /com1 / temp/tagged. / team /. Xplosion /fxp (inaccessible, à moins de connaître le chemin entier)

Voila c'est à peu près les principales astuces pour protéger son travail, sachant que les serveurs "non-deletable" sont plus sur, il n'y a que le Sysop qui peut les effacer et pour cause il est l'administrateur du ftp)

Notez que certains serveurs n'acceptent pas ces manipulation ce qui est un handicape, toutefois ils sont toujours utilisables.

7. Le test de FXP :

Qu'est ce que le FXP ?

Le FXP vient de File eXchange Protocol et il permet de copier des fichiers d'un serveur FTP à un autre en utilisant un client FXP. Habituellement, vous transférer des fichiers en utilisant le protocole FTP entre votre machine et un serveur FTP, et la vitesse maximum de transfert dépend de la vitesse de votre connexion Internet(par exemple : 56k, câble, ADSL, T1) Quand vous transférer des fichiers entre 2 serveurs en utilisant un client FXP, la vitesse maximum de transfert ne dépends pas de votre connexion mais uniquement de la connexion entre les 2 serveurs, qui est généralement plus rapide que votre propre connexion ce qui permet de propager facilement et rapidement une release. Par contre, parce que c'est une connexion directe, vous ne pourrez pas voir la progression, ni la vitesse de transfert des fichiers.
Bien que faire du FXP soit très facile, il y a quelques restrictions pour transférer les fichiers.
Les 2 serveurs doivent supporter le mode PASV et doivent permettre d'utiliser des commandes PORT vers d'autres serveurs. Le client FXP dit au FTP destinataire d'attendre une connexion en envoyant une commande PASV. Le FTP source se connecte alors sur le port de données fourni par le serveur destinataire(après une commande PASV réussie). Donc toutes les données vont directement de la source au destinataire et les deux serveurs reporte uniquement les messages de statuts et d'erreurs/succès au client FXP.

Pourquoi FXP ?

Le grand avantage de FXP et que ça ne passe pas par votre bande passante, alors il est même possible de FXP avec une connexion 57k, et de faire des transferts autour de 500k/s (pour les bons serveurs) qui ne sont possibles qu'en connexion d'un serveur avec un autre.

Le but d'FXP est de se faire un DUMP qu'on ne postera pas, où l'on récupérera tous les fichiers qui nous intéressent (ISO, Ripz, Appz …) en vu de les renvoyer vers des Pubs que l'on postera dans le forum approprié du site de son group FXP favoris.

Il est possible de FXP qu'entre certains serveurs. Je m'explique:

Le transfert est possible entre un serveur NT et un serveur Unix, et entre 2 serveurs Unix, sachant que l'un des 2 serveurs doit être FXPable (indispensable). Le transfert n'est pas possible entre deux serveurs NT.
Pour effectuer le transfert entre 2 serveurs NT il faut passer par un "Wingate" (à configurer dans la section proxy du client fxp pour ma part je n'en utilise pas car le transfert est très lent et donc a fuir)
Sachez que tous les pubs ne sont pas fxpables mais il suffit généralement que l'un des deux le soit pour faire un échange de données.

Un serveur fxp peut etre fxpable en send , en recive ou les deux mais ces dernier sont chasse garde on les appelle les dumps.

De quoi a ton besoin ?

Tout d'abord nous avons besoins d'un logiciel client ftp qui gère le FXP le logiciel le plus couramment utilisé pour faire du FxP est FlashFXP vous prouver le télécharger a l'adresse suivante http://www.flashfxp.com/ . On peut aussi utiliser SmartFTP mais ici pour notre exemple nous utiliserons FlashFXP

Pour commencer, il vous faut trouver 2 serveurs FTP avec un accès anonyme (reportez vous a la page comment scanner) l'un d'entre eux doit être fxplable

Exemple du tutorial:

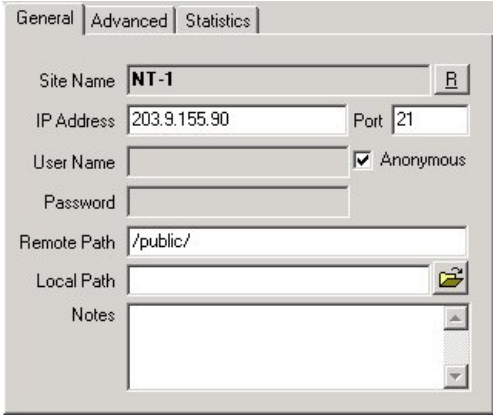
203.9.155.90

DIR: /public/
DELETE STATS: deletable
RUNNING OS: Windows_NT version 4.0
RESUMABLE: No
FXP STATS: non-FXPable
SEND SPEED: 4872,57 bytes/s

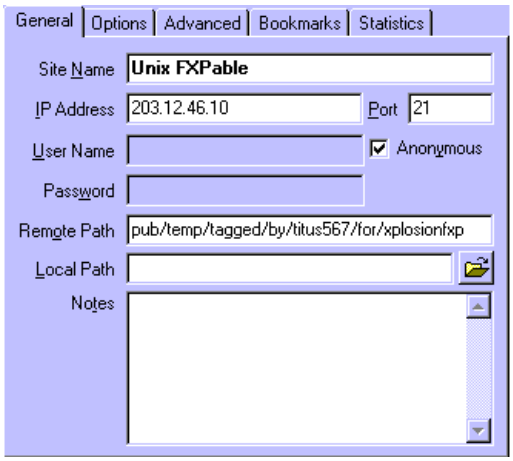
203.12.46.10

DIR: /pub/temp/tagged/by/titus567/for/xplosionfxp
DELETE STATS: nondeletable
RUNNING OS: UNIX Type: L8
RESUMABLE: Yes
FXP STATS: FXPable ----------> Important
SEND SPEED: 5112,81 bytes/s

Une fois que vous avez vos 2 serveurs, il vous faut configurer FlashFXP (en fait, juste ajouter les 2 serveurs).

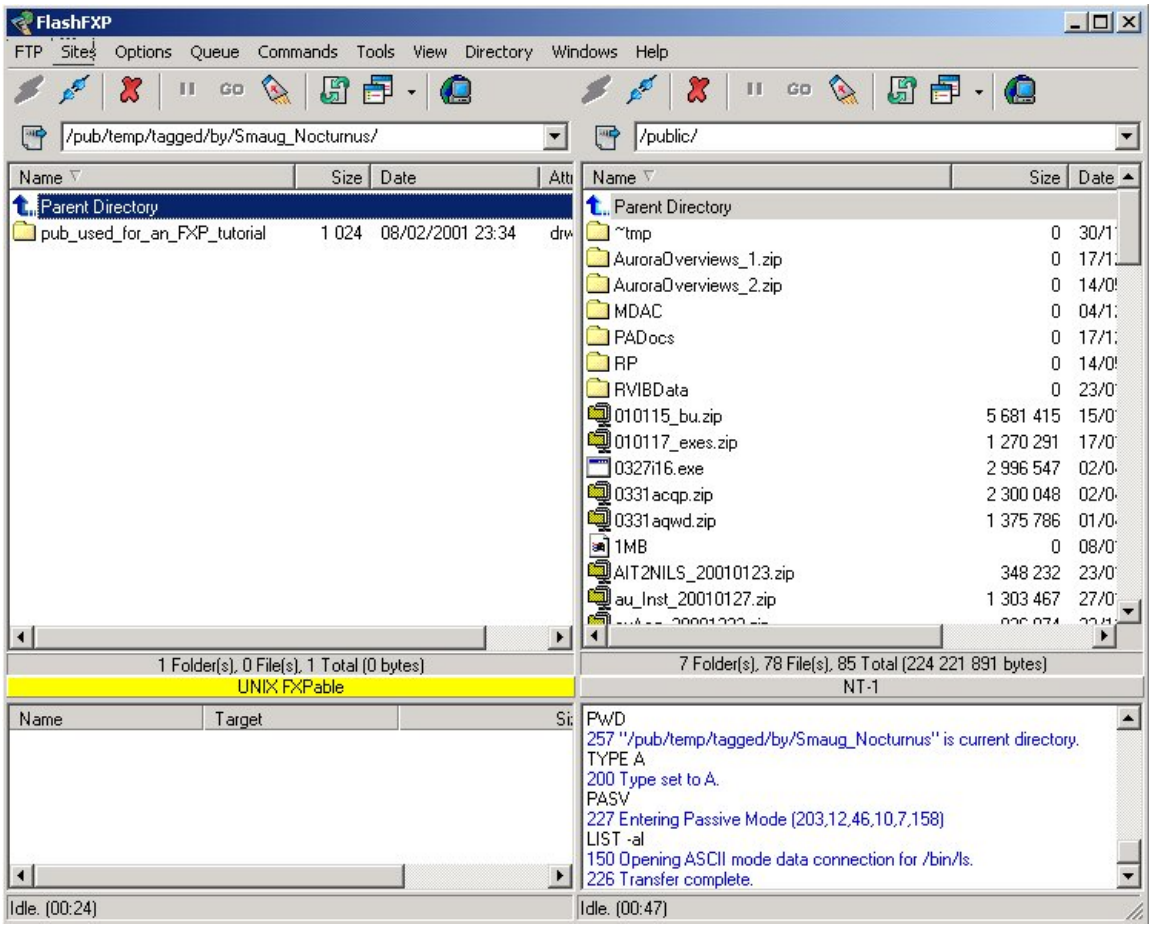


Allez dans "Sites"-->"Sites Manager" (F4).
Là cliquez sur le bouton "New Site" et entrez son nom, dans le cas présent NT-1, puis son IP et son chemin d'accès et cochez la case "Anonymous" puis cliquez sur le bouton "Apply".



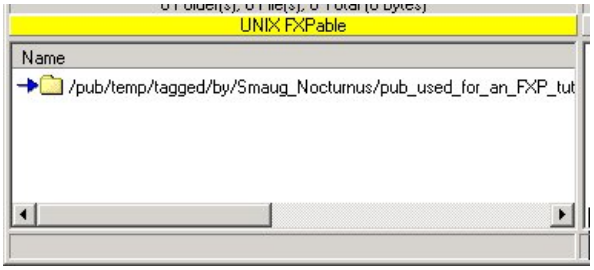
Ensuite faites de même avec le deuxième serveur: Unix FXPable
N' oubliez pas d'appuyer sur Apply puis enfin sur Close.

Une fois vos serveurs ajoutés, connectez vous à l'un dans la fenêtre de gauche (en cliquant sur l'éclaire et en le sélectionnant) puis au second dans la fenêtre de droite de la même façon.
Vous obtenez quelque chose comme ceci :



Il se peut que vous ayez le contenu d'un dossier de votre disque dans l'une des fenêtres, dans ce cas cliquez sur le bouton "Toggle Local View" : se trouvant au-dessus de la fenêtre concernée.

Il ne vous reste plus qu'a faire un "glissé déposé" de l'un vers l'autre (le serveur FXPable s'occupera du reste). Vous avez un listing des opérations dans le cadre inférieur gauche de FlashFXP comme le montre le schéma.



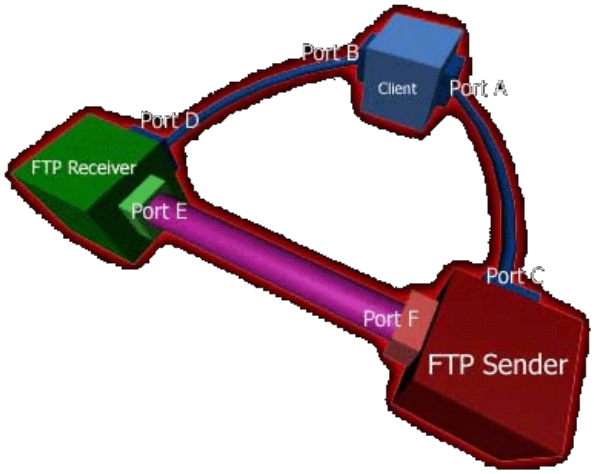
Notez qu'il est impossible de voir le pourcentage du transfert effectué d'un fichier, vous ne saurez qu'une fois le transfert terminé sauf si se sont des dump (fxpable en send et en recive)

Il est possible d'interrompre un transfert, et de le reprendre que si les deux serveurs sont résumable.
Sachez également que si vous quittez FlashFXP les transferts sont interrompus.

Voili voila c'est easy non? Sachez quand même qu'en général on trouve 99% de sites non FXPable (NT serveurs). Donc les serveurs FXPables sont rares gardez les pour vous pour vous en servir comme relai
Le Top du Top étant de tomber sur un Serveur SUN OS qui est FXPable vers tous les types de serveurs !!! le Graal pour tout le monde ceux la vous les gardez jalousement pour vous. Vienne en 2ème position les Unix souvent Fxpable puis les NT qui le permettent rarement.Donc gardez les sites FXPable pour vous sauf les undeletables que vous pouvez utiliser pour faire des post sur votre board préférées.

Dernière chose, pour être plus ou moins sûr que les pubs que je poste tiennent, je laisse 1 à 2 jours s'écouler entre le scanning proprement dit et le tagging, comme ça, si le pub ne tient déjà plus, il s'agissait certainement d'une machine personnelle et donc je le vire. Et 1 à 2 jours entre le tagging et le test de FXP et si le tag est déjà delete, cela signifie que le sysop a capté ou qu'un scanner crétin est passé par là, donc c'est mauvais et je le vire aussi

Pour ceux qui veulent pousser plus loin la compréhension voici un schéma explicatif qui montre les ports utilisés lors du transfert avec la description de chaque port.



Port A= Port défini par le FTP Sender pour les transfert des commandes.
Port B= Port défini par le FTP Receiver pour les transfert des commandes.
Port C= Port local du FTP Sender (Port 21 en général)
Port D= Port local du FTP Receiver(Port 21 en général)
Port E= Port défini par FTP Receiver lors de la commande PASV sur lequel FTP sender va se connecter grâce à la commande PORT.
Port F= Port local de données ouvert pour le transfert.

En même temps, voici ce que l'on peut observer en local pendant le transfert:

	Local	Remote
FTP sender	Port 20	Port P
FTP receiver	Port P	Port 20

Le sender a son port 20 ouvert et envoie les données sur le port P du receiver.

Et bien oui se tutorial touche a sa fin après vous avoir consacre pas loin de trois jours de mon temps
Le travaille du scanneur est desormais fini, vous pouvez maintenant poster votre boulot dans la section scan de votre groupe de cette facon :

203.9.155.90

DIR: /public/. tagged/for/xplosionfxp/~/.scanned/by/titus567/
DELETE STATS: deletable
RUNNING OS: Windows_NT version 4.0
RESUMABLE: No
FXP STATS: non-FXPable
SEND SPEED: 4872,57 bytes/s

203.9.155.90

DIR: /public/
DELETE STATS: deletable
RUNNING OS: Windows_NT version 4.0
RESUMABLE: No
FXP STATS: non-FXPable
SEND SPEED: 4872,57 bytes/s
TAG: /public/.tmp/com1/.tmp/com2/.tmp/com3/.tmp/ ~/ --==Scanned And Tagged==--/--==By titus567 For Xplosion FXP Team==-- /

Une fois taggué comme ceci, il reste plus qu'a uploader !!!! mais avant de finir le tutorial par l'upload voyons le respect de certaine règles.

8. Règles d'or a respecter absolument :

Vérifier toujours les TAGS avant de prendre possession du Pub, certain disent que si un tag est plus vieux que 2 semaines, et est inactif, et bien, vous pouvez prendre possession du serveur et effacer le tag.
Personnellement je pense que deux mois est vraiment le minimum,
Pour ceux qui sont plus ancien que deux mois, alors c'est bon, mais avant vérifiez qu'il n'y a rien dedans (s'il n'y a rien c'est bon), s'il y a encore quelque chose, mais que ça date, laisser un petit message est demander si vous pouvait prendre possession du pub.

N'effacez jamais rien sur les Pubs des autres

Toujours tagguer un pub avant de le rendre public

Donnez toujours du crédit au scanneur qui vous fournit le Pub, en lui postant un petit message de remerciement sur le forum. ça fait plaisir, ça ne coûte rien, de plus il continuera à vous fournir des pubs car je rappelle que sans scanneur pas de pub.

Ne repostez jamais le Pub de quelqu'un d'autre

N'uploader pas de fichier sur le pub que quelqu'un a déjà uploader et poster dans le forum sans lui demander la permission mais si il fait partie de votre team.

Si vous téléchargez quelque chose sur un pub, postez une réponse dans le forum à la personne qui la créé, ça fait plaisir, ça ne coûte rien, et il continuera à en créer d'autres.

Ne vous plaignez jamais d'une connexion lente, ce n'est pas la faute de la personne qui a fait le Pub, ça peut être vous, soit le Pub et trop loin (à l'autre bout du monde) ou bien encore il est surchargé. De toute façon la personne s'est donnée du mal, ne critiquez pas son travail.

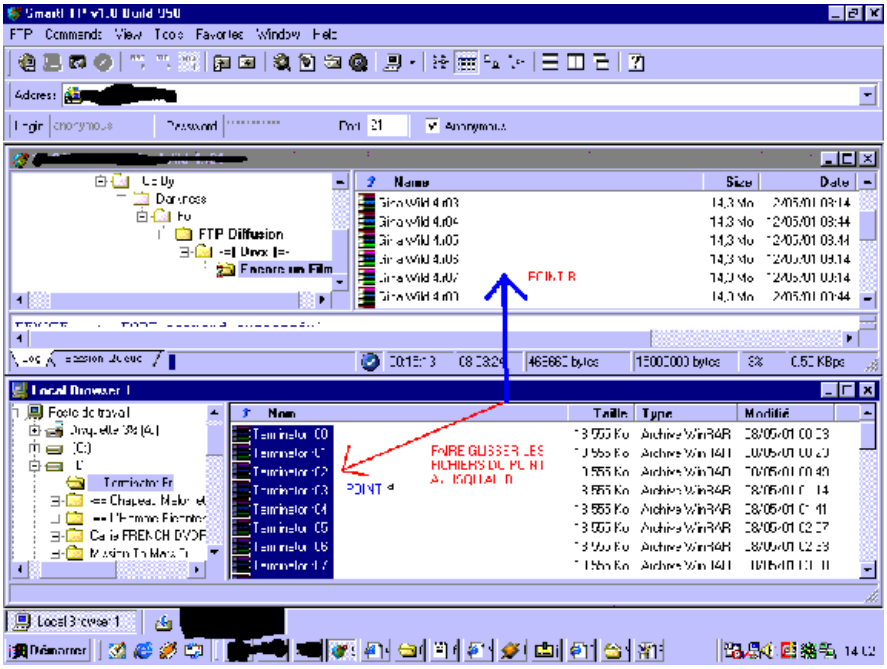
9. **Uploader :**

Une fois votre tag apposé, vous allez créer un autre répertoire nommé 'up by titus567' et dans lequel vous uploader par la suite.

Exemple: /.temp/. tagged by titus567/.for xplosionfxp/up by titus567/

Cela est très important car une fois vos fichiers balancés, et que vous voudrez poster votre beau travail sur une board, ca permettra de savoir que vous etes bien le 'propriétaire' du post et du boulot et non pas un leecheur ou pub stealer voleur de post.

Pour uploader utiliser SmartFTP comme ceci :



cliquer sur le bouton qui a l' icône du post de travail (local browser) cela vous ouvre un explorateur
puis chercher dans l'explorateur les fichier a upper a la manières du "glisser/deposé" sélectionnés les fichiers a upper puis mettez les sur le répertoire du ftp voulu.
Poster votre job

Ca y c'est la fin, vous avez uploader pleins de beaux fichiers et vous voulez que d'autres en profitent ...
Rendez vous sur votre board préférée, repérez la bonne section et poster !

vous devrez indiquer l'IP de votre ftp , par exemple : 102.40.56.140 (vous précipitez pas c'est inventé !)

ainsi que le path où l'on peut trouver les fichiers, par exemple : /tmp/_vti_pvt/scan-and-tag-by-titus567/up-by-titus567/appz/

Indiquez aussi le contenu c'est plus pratique pour savoir ce qui y a dedans ainsi les personne intéresser pourront faire un reply de remerciement

Faites attention, sur certaines board , il vous faudra indiquer l'IP et le path dans une section spéciale afin d'éviter les leecheurs.

L'IP sera ainsi masquée et ne sera dévoilée qu'apres un reply des gens intéressés...

Voilà fin de la leçon, attendez les replys !!!

Je n'ai pas la science infuse j'ai essayer de faire ce tutorial d'après mes connaissance toute critique sera la bienvenue dans l'amélioration du tutorial.

J'espère que ce tutorial vous a apporter quelque chose et n'oublier pas le savoir ne vaut que s'il est partagés par tous.

Les newbies d'aujourd'hui seront l'élite de demain